AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of dynamically protecting access to a first network, comprising:

receiving, in a system, a data unit containing a source address indicating a source of a data unit;

matching the source address with information stored in the system; [[and]]

enabling entry of the data unit to the first network for communication to a destination device on the first network if the source address matches the information stored in the system and denying entry of the data unit to the first network if the source address does not match the information stored in the system,

wherein the destination device is separate from the system;

determining whether the data unit contains an identifier of a codec type that matches a stored codec type; and

indicating occurrence of an attack of the first network in response to determining that the identifier is of a codec type that does not match the stored codec type.

2. (Original) The method of claim 1, wherein matching the source address with the information comprises matching the source address with one or more entries of a network address translation mapping table.

3. (Original) The method of claim 1, wherein matching the source address comprises matching an Internet Protocol address.

4. (Cancelled)

5. (Currently Amended) A method of dynamically protecting access to a first network, comprising:

receiving, in a system, a data unit containing a source address indicating a source of [[a]] the data unit;

matching, by an address filter in the system, the source address with information stored in the system;

enabling, by the address filter, entry of the data unit to the first network if the source address matches the information stored in the system and denying entry of the data unit to the first network if the source address does not match the information stored in the system; and

determining, by a protocol filter, if the data unit contains a payload according to a predetermined protocol, and denying, by the protocol filter, entry of the data unit if the data unit does not contain payload according to the predetermined protocol.

6. (Original) The method of claim 5, wherein determining if the data unit contains a payload according to the predetermined protocol comprises determining if the data unit contains a payload according to a Real-Time Protocol or Real-Time Control Protocol.

7. (Previously Presented) A method of dynamically protecting access to a first network, comprising:

receiving, in a system, a data unit containing a source address indicating a source of a data unit;

matching the source address with information stored in the system;

enabling entry of the data unit to the first network if the source address matches the information stored in the system and denying entry of the data unit to the first network if the source address does not match the information stored in the system; and

storing profile information for a call session, and determining if an unauthorized access of the first network is occurring based on the profile information.

8. (Original) The method of claim 7, wherein storing the profile information comprises storing a threshold representing a maximum acceptable rate of incoming data units from an external network to the first network.

9. (Original) The method of claim 8, further comprising calculating a value for the threshold based on a frame size used in the call session.

10. (Original) The method of claim 8, wherein storing the profile information further comprises storing a pattern expected in incoming data units.

11. (Original) The method of claim 10, wherein storing the pattern comprises storing a codec type used in the call session.

12. (Original) The method of claim 8, further comprising generating an alarm if the system detects a rate of incoming data units from the external network to the first network exceeding the threshold.

13. (Original) The method of claim 8, further comprising denying further transport of incoming data units from the external network to the first network for the call session if the system detects a rate of incoming data units from the external network to the first network exceeding the threshold.

14. – 15. (Cancelled)

16. (Currently Amended) An article comprising at least one storage medium containing instructions for protecting a first network, the instructions when executed causing a system to:

determine if a rate of incoming data units from an external network to the first network exceeds a predetermined threshold in a given call session;

perform a security action if the determined rate of incoming data units exceeds the predetermined threshold, wherein performing the security action comprises generating a report that an attack is occurring; and

store plural thresholds for corresponding plural call sessions.

17. (Previously Presented) An article comprising at least one storage medium containing instructions for protecting a first network, the instructions when executed causing a system to:

determine if a rate of incoming data units from an external network to the first network exceeds a predetermined threshold in a given call session;

perform a security action if the determined rate of incoming data units exceeds the predetermined threshold; and

calculate the predetermined threshold based at least in part on a frame size used in the call session.

18. (Cancelled)

19. (Previously Presented) An article comprising at least one storage medium containing instructions for protecting a first network, the instructions when executed causing a system to:

determine if a rate of incoming data units from an external network to the first network exceeds a predetermined threshold;

perform a security action if the determined rate of incoming data units exceeds the predetermined threshold; and

determine if each incoming packet has a predetermined pattern,

wherein the instructions when executed cause the system to determine if each incoming packet has the predetermined pattern by checking if each incoming packet has an indication of a predetermined codec type.

20. (Cancelled)

21. (Currently Amended) A system for use in communications between a first network and an external network, comprising:

a storage module to store a threshold value for a communications session, the threshold value representing an acceptable rate of incoming data units from the external network to the first network; and

a controller adapted to deny further entry of data units from the external network to the first network in the communications session and to generate a report of an attack from the external network in response to the controller detecting that the rate of incoming data units exceeds the threshold value,

the storage module to further store address information, wherein the controller is adapted to compare a source address of an incoming data unit with the address information stored in the system and to deny further entry of the incoming data unit if the source address does not match the address information stored in the system.

22. (Original) The system of claim 21, wherein the address information comprises a network address translation table.

23. (Original) The system of claim 22, wherein the network address translation table comprises a network address and port translation table.

24. (Original) The system of claim 21, wherein the controller is adapted to further check if the incoming data unit contains a Real-Time Protocol or Real-Time Control Protocol payload, and to deny further entry of the incoming data unit if the incoming data unit does not contain a Real-Time Protocol or Real-Time Control Protocol payload.

25. (Previously Presented) A system for use in communications between a first network and an external network, comprising:

a storage module to store a threshold value for a communications session, the threshold value representing an acceptable rate of incoming data units from the external network to the first network; and

a controller adapted to deny further entry of data units from the external network to the first network in the communications session in response to the controller detecting that the rate of incoming data units exceeds the threshold value,

the storage module to further store a codec type for the communications session, wherein the controller is adapted to deny entry of an incoming data unit if the incoming data unit does not contain an indication of the codec type.

26. (New) The article of claim 17, wherein performing the security action comprises generating a report that an attack is occurring.